

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

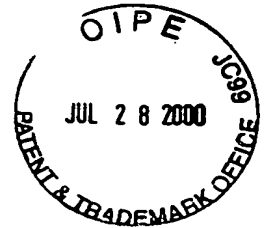
- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 5月10日

出 願 番 号

Application Number:

平成11年特許願第128197号

出 願 人

Applicant (s):

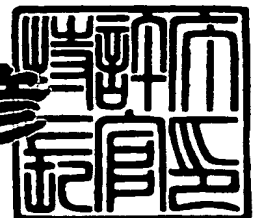
松下電器産業株式会社

RECEIVED  
OCT-2 2000  
TC 2700 MAIL ROOM

2000年 3月 3日

特許庁長官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3012867

【書類名】	特許願
【整理番号】	2032410063
【提出日】	平成11年 5月10日
【あて先】	特許庁長官殿
【国際特許分類】	G11B 7/00
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式 会社内
【氏名】	東海林 衛
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式 会社内
【氏名】	大嶋 光昭
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式 会社内
【氏名】	石田 隆
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式 会社内
【氏名】	中村 敦史
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式 会社内
【氏名】	謝花 正司
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式 会社内
【氏名】	中田 浩平

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 大原 俊次

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【ブルーフの要否】 不要

【書類名】 明細書

【発明の名称】 暗号化コンテンツ記録方法および光ディスク

【特許請求の範囲】

【請求項 1】 第 1 のディスク情報が記録されている第 1 情報領域と、個々のディスクを識別するための第 2 のディスク情報が記録されている第 2 情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域を有することを特徴とする光ディスク。

【請求項 2】 第 2 情報領域は、前記第 1 情報領域内に記録されていることを特徴とする請求項 1 記載の光ディスク。

【請求項 3】 第 2 情報領域は、前記第 1 情報領域内の記録膜を、半径方向に長い形状でかつ複数個、部分的に除去することにより記録されていることを特徴とする請求項 2 記載の光ディスク。

【請求項 4】 第 1 のディスク情報が記録されている第 1 情報領域と、個々のディスクを識別するための第 2 のディスク情報が記録されている第 2 情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域を有する光ディスクの前記データ領域にコンテンツを記録する際に、少なくとも前記第 2 のディスク情報を用いた演算により、復号して再生することができるよう暗号化して記録することを特徴とする暗号化コンテンツ記録方法。

【請求項 5】 データ領域内に、暗号化されて記録されたデータを解読するための鍵情報を記録する鍵情報記録領域を有することを特徴とする請求項 1 記載の光ディスク。

【請求項 6】 第 1 のディスク情報が記録されている第 1 情報領域と、個々のディスクを識別するための第 2 のディスク情報が記録されている第 2 情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域と、前記データ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域を有する光ディスクの、前記データ領域にコンテンツを記録する際に、少なくとも前記第 2 のディスク情報と、前記鍵情報を用いた演算により、復号して再生することができるよう暗号化して記録することを特徴とする暗号化コンテンツ記録方法。

【請求項 7】 第 1 のディスク情報は、微少な凹凸ピットにより構成されていることを特徴とする請求項 1 記載の光ディスク。

【請求項 8】 第 1 のディスク情報は、微少な凹凸ピットにより構成されていることを特徴とする請求項 4 または 6 記載の暗号化コンテンツ記録方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、暗号化コンテンツ記録方法および書き換え型もしくは追記型の光ディスクに関する。

【 0 0 0 2 】

【従来の技術】

近年、再生専用光ディスク、特に CD-ROM の普及に伴い、CD-ROM を用いたソフト流通システムが実用化されている。この場合 CD-ROM を受け取ったユーザは、同梱のパスワードをパソコンから入力することにより、CD-ROM に予め記録されている暗号を解読する、もしくは暗号化されているコンテンツを解読するといった方法が一般的である。

【 0 0 0 3 】

しかしながら CD-ROM の場合、ディスク上に追記記録できないため各ディスクの ID は個別に設定できない。従って 1 つのパスワードが全てのディスクの暗号を解読してしまうことになり、ディスクが不正にコピーされても、コンテンツの解読が可能であった。

【 0 0 0 4 】

この課題を解決するために、光ディスクのピット部にバーコードを重ね書きするための追記領域（以下 B C A 領域と略す）を設け、光ディスク製造時に B C A 領域にディスク毎に異なる ID を記録しておく方法が提案されている（国際公開番号 WO 9 7 / 1 4 1 4 4 ）。

【 0 0 0 5 】

この方法によると、パスワードはディスク ID により異なるので、1 つのパスワードは 1 枚のディスクの暗号しか解読することができなくなり、コンテンツが

不正にコピーされてもディスク I D の情報が欠落しているため、コンテンツは解読されなくなる。

【 0 0 0 6 】

【発明が解決しようとする課題】

一方、インターネット等のネットワーク手段によりソフトを入手する場合には、再生専用光ディスクではなく、書き換え型の光ディスクを用いる方法が有望視されているが、書き換え型の光ディスクを用いたソフト流通システムの詳細については未だ確立されていない。

【 0 0 0 7 】

本発明は上記課題を鑑み、簡単なシステムで、ユーザ側の不正コピーを防止しつつ、ネットワークもしくは電波により発信されたコンテンツを光ディスクへ記録するための、暗号化コンテンツ記録方法を提供することを目的とする。

【 0 0 0 8 】

【課題を解決するための手段】

この課題を解決するために本発明の光ディスクは、第 1 のディスク情報が記録されている第 1 情報領域と、個々のディスクを識別するための第 2 のディスク情報が記録されている第 2 情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域を有する。

【 0 0 0 9 】

また、この課題を解決するために本発明の光ディスクの第 2 情報領域は、前記第 1 情報領域内に記録されている。

【 0 0 1 0 】

また、この課題を解決するために本発明の光ディスクの第 2 情報領域は、前記第 1 情報領域内の記録膜を、半径方向に長い形状でかつ複数個、部分的に除去することにより記録されている。

【 0 0 1 1 】

また、この課題を解決するために本発明の暗号化コンテンツの記録方法は、第 1 のディスク情報が記録されている第 1 情報領域と、個々のディスクを識別するための第 2 のディスク情報が記録されている第 2 情報領域と、光ビームを照射す

ることにより情報の記録が可能なデータ領域を有する光ディスクの前記データ領域にコンテンツを記録する際に、少なくとも前記第 2 のディスク情報を用いた演算により、復号して再生することができるように暗号化して記録する。

## 【 0 0 1 2 】

また、この課題を解決するために本発明の光ディスクは、データ領域内に、暗号化されて記録されたデータを解読するための鍵情報を記録する鍵情報記録領域を有する。

## 【 0 0 1 3 】

また、この課題を解決するための本発明の暗号化コンテンツの記録方法は、第 1 のディスク情報が記録されている第 1 情報領域と、個々のディスクを識別するための第 2 のディスク情報が記録されている第 2 情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域と、データ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域を有する光ディスクの前記データ領域にコンテンツを記録する際に、少なくとも前記第 2 のディスク情報と、前記鍵情報を用いた演算により、復号して再生することができるように暗号化して記録する。

## 【 0 0 1 4 】

また、この課題を解決するための本発明の光ディスクは、第 1 のディスク情報が微少な凹凸ピットにより構成されている。

## 【 0 0 1 5 】

また、この課題を解決するための本発明の暗号化コンテンツの記録方法は、第 1 のディスク情報が微少な凹凸ピットにより構成されている。

## 【 0 0 1 6 】

## 【発明の実施の形態】

本発明の請求項 1 に記載の発明の光ディスクは、第 1 のディスク情報が記録されている第 1 情報領域と、個々のディスクを識別するための第 2 のディスク情報が記録されている第 2 情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域を有するものであり、従来の光ディスクに、前記光ディスクを識別する情報を付加することにより、光ディスクの管理を容易に実現することが



できる。

【0017】

本発明の請求項2に記載の発明によると、第2情報領域は、前記第1情報領域内に記録されているものであり、第1情報領域を再生する光ピックによって再生することができる。

【0018】

本発明の請求項3に記載の発明によると、第2情報領域は、前記第1情報領域内の記録膜を、半径方向に長い形状でかつ複数個、部分的に除去することにより記録されているものであり、容易に前記第2情報が改ざんされることを防止することができる。

【0019】

本発明の請求項4に記載の発明によると、暗号化コンテンツの記録方法は、第1のディスク情報が記録されている第1情報領域と、個々のディスクを識別するための第2のディスク情報が記録されている第2情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域を有する光ディスクの前記データ領域にコンテンツを記録する際に、少なくとも前記第2のディスク情報を用いた演算により、復号して再生できるように暗号化して記録するものであり、特定の1枚のディスクにしか存在しない光ディスク識別情報により暗号化することにより、コンテンツの不正なコピーを防止することができ、著作権が保護できるという効果がある。

【0020】

本発明の請求項5に記載の発明の光ディスクは、データ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域を有するものであり、暗号化されて記録されたコンテンツを解読する際に鍵情報が必要なシステムにおいて、鍵情報記録領域に鍵情報が一度記録されることにより、再生する度に鍵情報を入力する必要がなくなるという効果がある。

【0021】

本発明の請求項6に記載の発明によると、暗号化コンテンツの記録方法は、第1のディスク情報が記録されている第1情報領域と、個々のディスクを識別する

ための第 2 のディスク情報が記録されている第 2 情報領域と、光ビームを照射することにより情報の記録が可能なデータ領域と、データ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域を有する光ディスクの前記データ領域にコンテンツを記録する際に、少なくとも前記第 2 のディスク情報と、前記鍵情報を用いた演算により、復号して再生することができるように暗号化して記録するものであり、暗号化されたコンテンツを別の光ディスクにコピーされても、不正に再生されることはなく、暗号化されたコンテンツをコピーした光ディスクを再生する際には必ず課金が伴うことから著作権を保護することができる。

## 【 0 0 2 2 】

本発明の請求項 7 と 8 に記載の発明によると、第 1 のディスク情報は、微少な凹凸ピットにより構成されるものであり、ディスクを識別するための第 2 のディスク情報が、前記凹凸ピット上に記録されることにより、容易に第 2 のディスク情報が改ざんされることを防止することができる。

## 【 0 0 2 3 】

さらに第 1 のディスク情報と第 2 のディスク情報が隣接していることにより、第 1 の情報を再生する際に、第 2 の情報も続けて再生することができる、もしくは第 2 の情報を再生する際に、第 1 の情報を続けて再生することができるので、例えばディスクを起動する際に CPU が速やかにディスクを識別するための第 2 の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

## 【 0 0 2 4 】

以下本発明の実施の形態における暗号化コンテンツ記録再生方法について図面を参照しながら説明する。

## 【 0 0 2 5 】

## (実施の形態 1)

図 1 は本発明による第 1 の実施の形態の光ディスクの平面図である。

## 【 0 0 2 6 】

図 1 において 1 0 1 は書き換え型もしくは追記型の光ディスク（以下光ディス

ク)、102はディスク情報を凹凸ピットで記録してあるコントロールデータ領域、103はユーザがデータを記録するデータ領域、104はディスクIDを記録してあるBCA領域である。

【0027】

BCA領域104では、コントロールデータ領域102の内周部分の凹凸ピット上の記録膜が、105の様に半径方向に長い形状でかつ複数個、部分的にYAGレーザなどのパルスレーザでトリミングされている。

【0028】

図2はBCA領域104を再生したときの出力信号の説明図である。また図3はBCA領域104を再生する回路であり、301は光ピックアップ、302はプリアンプ、303はローパスフィルタ、304は二値化回路、305は復調回路である。

【0029】

光ピックアップ301から出力されるレーザ光は光ディスク101のBCA領域104を照射し、その反射光がプリアンプ302で増幅されて信号201が得られる。

【0030】

信号201はコントロールデータ領域102の凹凸ピットによる信号であるが、202、203、204はパルスレーザによるトリミングで、記録膜が取り除かれて、凹凸ピットによる信号が欠落している部分である。なおトリミングはディスク製造者によって行われる。

【0031】

信号201はローパスフィルタ303に入力されて、凹凸ピットによる変調信号が除去された後に、二値化回路304に入力され、通常コントロールデータ領域の信号を二値化するスライスレベル205ではなく、スライスレベル206によって二値化されて信号207が得られる。二値化回路304の出力信号は、復調回路305で復調されてディスクID信号306が得られる。

【0032】

以上の様に、光ディスクを識別する情報を付加することにより、光ディスクの

管理を容易に実現することができる。またBCA領域が凹凸ピット上に記録されることにより、BCA領域内の光ディスクを識別する情報が容易に改ざんされることを防止することができる。

#### 【0033】

さらにコントロールデータ領域102とBCA領域104が隣接していることにより、コントロールデータ領域102を再生する際に、BCA領域104も続けて再生することができる、もしくはBCA領域104を再生する際に、コントロールデータ領域102を続けて再生することができるので、例えばディスクを起動する際にCPUが速やかにディスクを識別するためのBCA領域104の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

#### 【0034】

なお本実施の形態のBCA領域104は、コントロールデータ領域102の内周部分の凹凸ピット上の記録膜をトリミングしているが、書き換え型もしくは追記型の光ディスクを構成する記録膜は、再生専用の光ディスクにおける反射膜に対して熱による影響を受けやすい。コントロールデータ領域102の内周部分をトリミングすることにより、外周部分をトリミングする場合に比べて、トリミングの際に発生する熱からデータ領域103を保護することができる。

#### 【0035】

なおトリミング前のBCA領域104に記録されているデータが、コントロールデータ領域102に記録されていても良い。BCA領域104に記録されているデータが、コントロールデータ領域102にも記録されていることにより、トリミングを行ってもコントロールデータ領域102の前記データを保護することができる。

#### 【0036】

さらに前記データがBCA領域104から、コントロールデータ領域102まで連続して繰り返し記録されている場合には、コントロールデータ領域102の前記データを見つけることによって、BCA領域104の位置を予想することができる。

## 【0037】

次に、以上の様なBCA領域を有する光ディスクに、ネットワークを通して、ディスクIDで暗号化されたコンテンツを記録する手順を述べる。図4はBCA領域を有する書き換え型もしくは追記型の光ディスクを用いて暗号化コンテンツを記録する際のブロック図である。

## 【0038】

図4において、101は光ディスク、301は光ピックアップ、401はBCA再生部、402はディスクID信号、403、404はインターフェース、405はネットワーク、406は暗号化部、407は映像ソフト等のコンテンツ、408は暗号化エンコーダ、409は暗号化コンテンツ、410は記録再生装置、411は記録回路、412はデータ再生部、413は暗号デコーダである。

## 【0039】

まず、光ピックアップ301から出力されるレーザ光がRAMディスク101のBCA領域104を照射し、その反射光がBCA再生部401に入力され、BCA再生部401はディスクID信号402を出力し、インターフェース403、404とネットワーク405を介して、暗号化部406に送られる。

## 【0040】

暗号化部406では、コンテンツ407が記録される光ディスク101のディスクID信号402が暗号を解く復号鍵となるように、暗号化エンコーダ408において暗号化もしくは映像音声用のスクランブルを行う。

## 【0041】

なお本実施の形態では、暗号化処理について、コンテンツ407をディスクID信号402を暗号鍵として暗号化すると表現しても同意とする。

## 【0042】

また本実施の形態においては、暗号化や復号化を錠と鍵の関係で考え、前記錠を前記鍵で閉めることを暗号化とし、前記錠を前記鍵で開けることを復号化とする。従って暗号化と復号化で実際の演算は異なるが、暗号化するための鍵と復号化するための鍵は、同一であるとする。

## 【0043】

なおコンテンツ407をC、ディスクID信号402をBCA、暗号化されたコンテンツ409をC[BCA]、暗号化処理を\*すると、 $C * BCA = C[BCA]$ と表記する。

## 【0044】

暗号化されたコンテンツ409は、インターフェース403、404とネットワーク405を介して記録再生装置410に送られ、記録回路411の出力信号に応じて光ピックアップ301により光ディスク101に記録される。

## 【0045】

次に、光ディスク101に暗号化されて記録された前記コンテンツを再生する際は、光ピックアップ301から出力されるレーザ光がデータ領域103の前記暗号化コンテンツが記録された領域を照射し、その反射光がデータ再生部412に入力され、データ再生部412の出力信号は暗号デコーダ413に入力される。

## 【0046】

一方で、光ピックアップ301から出力されるレーザ光は光ディスク101のBCA領域104を照射し、その反射光がBCA再生部401に入力され、BCA再生部401はディスクID信号402を出力し、出力信号は暗号デコーダ413に入力される。

## 【0047】

暗号デコーダ413では、入力されたディスクID信号402を鍵として、暗号化された信号の復号を行う。このときコンテンツが正規に光ディスク101に記録されている場合は、光ディスク101に記録されている暗号化コンテンツを復号するための鍵は、光ディスク101のディスクID信号であり、再生時にBCA再生部から出力されるディスクID信号も、光ディスク101のディスクID信号であるので、復号もしくはデスクランブルされたコンテンツが、暗号デコーダ413から出力される。なお復号化処理を#すると、 $C[BCA] \# BCA = C$ と表記される。コンテンツが映像情報の場合は例えばMP EG信号が伸長されて、映像信号が得られる。

## 【0048】

以上の様に、本実施の形態における暗号化は、ディスクIDを鍵としており、

ディスク ID は世の中に 1 枚しか存在しないため、1 枚の光ディスクにしか同じ暗号化コンテンツの記録ができないという効果がある。

【0049】

前記コンテンツ 407 を、例えば ID1 というディスク ID を持つ正規の光ディスクから、ID2 という別のディスク ID を持つ別の光ディスクにコピーして再生しようとした場合、BCA 再生部 401 からディスク ID 信号 402 として ID2 が出力される。しかし暗号化コンテンツは ID1 というディスク ID 信号で暗号化されているので、暗号デコーダ 413 で、暗号化コンテンツを復号することができない。

【0050】

なお、暗号化エンコーダ 408 はコンテンツの供給元ではなく、ネットワークに対して記録再生装置側にあり、暗号化エンコーダを搭載した IC カード等の形態であっても良い。

【0051】

また、前記光ディスク 101 はディスク ID のみで暗号化されているので、BCA 再生部と暗号デコーダを有する任意の光ディスク記録再生装置で再生することが可能である。

【0052】

以下本発明の異なる実施の形態における暗号化コンテンツ記録方法について図面を参照しながら説明する。

【0053】

(実施の形態 2)

図 5 は本発明による第 2 の実施の形態における、BCA 領域を有する書き換え型もしくは追記型の光ディスクを用いて暗号化コンテンツを記録する際のブロック図である。なお、第 1 の実施の形態と共通の部分は説明を簡略化する。

【0054】

図 5 において、501 は CATV 会社、502 は映画ソフト等のコンテンツ、503 は第 1 暗号鍵、504 は第 1 暗号化エンコーダ、505 は第 1 暗号化コンテンツ、506 は CATV デコーダ、507 は鍵発行センター、508 は CAT

Vデコーダ506のシステムID、509はコンテンツ502のタイトルコード、510は時間制限情報、511は記録許可コード、513は第1暗号デコーダ、101はBCA領域を有する書き換え型もしくは追記型の光ディスク（以下光ディスク）、514は光ディスク記録装置、515は光ディスク101のディスクID信号、516は第2暗号化エンコーダ、517は第2暗号化コンテンツ、518は記録回路、519はデータ再生部、520は第2暗号デコーダ、521はBCA再生部、522、524はICカード、523、526は会社識別信号である。

【0055】

まずCATV会社501は、映画ソフト等のコンテンツ502を第1暗号鍵503を用いて第1暗号化エンコーダ504にて暗号化し、第1暗号化コンテンツ505を生成し、ネットワークを介して各ユーザのCATVデコーダ506に送信する。

【0056】

ここでコンテンツ502をC、第1暗号鍵503をFK、第1暗号化コンテンツ505をC[FK]とすると、 $C * FK = C[FK]$ と表記される。

【0057】

CATVデコーダ506は、ネットワークを介して鍵発行センター507へ、CATVデコーダ506のシステムID508と、視聴もしくはRAMディスクへの記録を行いたい前記コンテンツのタイトルコード509を送る。

【0058】

なお、タイトルコード509はTVの画面に従って選択することにより入力しても良いし、直接キーボードから入力しても良いし、リモートコントローラー等から入力しても良い。従ってタイトルコード509は、ユーザが独自に入手していても良いし、第1暗号化コンテンツ505と共にCATVデコーダ506に送られてきても良いし、番組案内等の形態で第1暗号化コンテンツ505とは別の時間に予め送られていても良い。

【0059】

鍵発行センター507は、CATVデコーダ506のシステムID508、前



記コンテンツのタイトルコード 5 0 9、時間制限情報 5 1 0、記録許可コード 5 1 1 に対応する鍵 K 5 1 2 を記録許可コード 5 1 1 と共に CATV デコーダ 5 0 6 の第 1 暗号デコーダ 5 1 3 へネットワークを介して送信する。

【 0 0 6 0 】

なお時間制限情報 5 1 0 により、同一のコンテンツを時間を変えて複数回放送する場合を区別することができる。

【 0 0 6 1 】

ここで第 1 復号鍵を FK、CATV デコーダ 5 0 6 のシステム ID 5 0 8 を DID、時間制限情報 5 1 0 を TIME、記録許可コード 5 1 1 を COPY、コンテンツのタイトルコード 5 0 9 を T とするとき鍵 K は、 $FK = K * T * DID * TIME * COPY$  の関係を満たしている。

【 0 0 6 2 】

なお記録許可コード 5 1 1 は、例えば CATV 会社 5 0 1 が、放送するコンテンツが新作品か旧作品かを判断して、視聴のみ許可するのか、視聴、記録の両方を許可するのかを決定する。

【 0 0 6 3 】

第 1 暗号デコーダ 5 1 3 は鍵 K 5 1 2 と、前記コンテンツ 5 0 2 のタイトルコード 5 0 9 と、システム ID 5 0 8 と、記録許可コード 5 1 1 に加えて、時間情報 5 2 7 が時間制限情報 5 1 0 の条件を満たしていれば、第 1 暗号化コンテンツ 5 0 5 を復号し、映像信号の場合は、デスクランブルされた信号が出力され、TV で視聴できる。

【 0 0 6 4 】

ここで復号化処理を式で表すと、 $C[FK] \# (K * T * DID * TIME * COPY) = C[FK] \# FK = C$  となる。

【 0 0 6 5 】

なお、記録許可コード 5 1 1 が視聴のみ許可する場合は、光ディスク 1 0 1 に記録できないが、視聴、記録の両方を許可する場合は記録することができるので、以降でこの方法について説明する。

【 0 0 6 6 】

光ディスク記録装置 514 は、光ディスク 101 の B C A 領域 104 を再生し、ディスク I D 信号 515 が B C A 再生部 521 の出力信号として C A T V デコーダ 506 の第 2 暗号化エンコーダ 516 に送られる。

## 【0067】

第 2 暗号化エンコーダ 516 ではディスク I D 信号 515 を第 2 暗号鍵として用いて、第 1 暗号デコーダ 513 から出力されたコンテンツを第 2 暗号化エンコーダにて暗号化し、第 2 暗号化コンテンツ 517 を生成し、光ディスク記録装置に送信する。

## 【0068】

なお前記暗号化は第 1 暗号デコーダ 513 から第 1 暗号化コンテンツが復号されて出力されている間に限られる。

## 【0069】

ここで、第 1 暗号デコーダ 513 の出力信号であるコンテンツを C、第 2 暗号鍵であるディスク I D 信号 515 を B C A、第 2 暗号化コンテンツ 517 を C [ B C A ] とするとするとき、 $C * B C A = C [ B C A ]$  と表記される。

## 【0070】

光ディスク記録装置 514 に送られた第 2 暗号化コンテンツ 517 は、記録回路 518 により例えば 8-16 変調により変調されて、図示しない光ピックアップにより光ディスク 101 のデータ領域 103 に記録される。

## 【0071】

光ディスク 101 に暗号化されて記録された前記コンテンツを再生する際は、光ピックアップから出力されるレーザ光が光ディスク 101 の前記暗号化されたコンテンツが記録されている領域を照射し、その反射光がデータ再生部 519 に入力され、データ再生部 519 の出力信号は第 2 暗号デコーダ 520 に入力される。

## 【0072】

一方で、光ピックアップから出力されるレーザ光は光ディスク 101 の B C A 領域 104 を照射し、その反射光が B C A 再生部 521 に入力され、B C A 再生部 521 はディスク I D 信号 515 を出力し、出力信号は第 2 暗号デコーダ 520 に入力される。

【0073】

第2暗号デコーダ520では、入力されたディスクID信号515を鍵として、暗号化されたコンテンツの復号を行う。このときコンテンツが正規に光ディスク101に記録されている場合は、光ディスク101に記録されている暗号化コンテンツを復号するための鍵は光ディスク101のディスクIDであり、BCA再生部514から出力されるディスクID信号も、光ディスク101のディスクID信号であるので、復号もしくはデスクランブルされたコンテンツが、第2暗号デコーダ520から出力される。

【0074】

ここで復号化処理を式で記述すると、 $C[BCA] \# BCA = C$ となる。コンテンツが映像情報の場合は例えばMP EG信号が伸長されて、映像信号が得られる。

【0075】

また、前記光ディスク101はディスクID515のみで暗号化されているので、BCA再生部と第2暗号デコーダを有する任意の光ディスク記録装置で再生することが可能である。

【0076】

なお、暗号エンコーダで暗号化、暗号デコーダで複合化を説明したが、CPUの中のプログラムである暗号アルゴリズムおよび復号アルゴリズムを用いても良い。

【0077】

なお本実施の形態では、第2暗号化エンコーダ516ではディスクID信号515を第2暗号鍵として用いて暗号化したが、例えば各CATV会社毎に準備されたICカード522をCATVデコーダ506に装着して、ICカード内に記録されている会社識別信号523とディスクID信号515を組み合わせることで第2暗号鍵とし、第2暗号化エンコーダ516にて暗号化しても良い。

【0078】

ここで、第1暗号デコーダ513の出力信号であるコンテンツをC、第1の第2暗号鍵であるディスクID515をBCA、第2の第2暗号鍵である会社識別

信号 5 2 3 を CK、第 2 暗号化コンテンツ 5 1 7 を C [BCA, CK] とするとき、暗号化処理を式で記述すると、 $C * BCA * CK = C [BCA, CK]$  と表記される。

【 0 0 7 9 】

次に光ディスク 1 0 1 に暗号化して記録されたコンテンツを再生する際には、光ピックアップから出力されるレーザ光が光ディスク 1 0 1 の前記暗号化されたコンテンツが記録されている領域を照射し、その反射光がデータ再生部 5 1 9 に入力され、データ再生部 5 1 9 の出力信号は第 2 暗号デコーダ 5 2 0 に入力される。

【 0 0 8 0 】

一方で、光ピックアップから出力されるレーザ光は光ディスク 1 0 1 の BCA 領域 1 0 4 を照射し、その反射光が BCA 再生部 5 2 1 に入力され、BCA 再生部 5 2 1 はディスク ID 信号 5 1 5 を出力し、出力信号は第 2 暗号デコーダ 5 2 0 に入力される。

【 0 0 8 1 】

さらに光ディスク記録装置 5 1 4 に装着された IC カード 5 2 4 内の会社識別信号 5 2 6 が第 2 暗号デコーダ 5 2 0 に入力される。なお会社識別信号 5 2 6 は、IC カード 5 2 4 内に記録されていなくても良く、インストールによって光ディスク記録装置 5 1 4 内のメモリに記録されていても良いし、IC カード 5 2 2 内の会社識別信号 5 2 3 が入力されても良い。

【 0 0 8 2 】

第 2 暗号デコーダ 5 2 0 では、入力されたディスク ID 信号 5 1 5 と会社識別信号 5 2 6 を復号鍵として、暗号化された信号の復号を行う。このとき特定の CATV 会社 5 0 1 と正式に契約をし、コンテンツ 5 0 2 が正規に光ディスク 1 0 1 に記録されている場合は、光ディスク 1 0 1 に暗号化されて記録されている暗号化コンテンツの第 1 の復号鍵は、まさに再生しようとする光ディスク 1 0 1 のディスク ID 信号であり、第 2 の復号鍵は、契約した CATV 会社 5 0 1 から提供された IC カード 5 2 4 内の会社識別信号 5 2 6 であるので、復号もしくはデスクランブルされたコンテンツ 5 2 5 が、第 2 暗号デコーダ 5 2 0 から出力される。

【 0 0 8 3 】

復号化処理を式で記述すると、 $C[BCA, CK] \# (BCA * CK) = C$ となる。コンテンツ 5 2 5 が映像情報の場合は例えば M P E G 信号が伸長されて、映像信号が得られる。

【 0 0 8 4 】

また、前記光ディスク 1 0 1 はディスク I D 5 1 5 と会社識別信号 5 2 1 で暗号化されているので、前記コンテンツの提供元の C A T V 会社と契約を結んでいれば、BCA再生部と、第2暗号デコーダを有する任意の光ディスク記録再生装置で再生することが可能である。

【 0 0 8 5 】

逆に前記 C A T V 会社 5 0 1 と契約していなければ、会社識別信号を入手できないので、コンテンツを再生することができず、契約済みのユーザとの差別化を可能にする。

【 0 0 8 6 】

また本実施の形態では、各ユーザは自宅の C A T V デコーダに光ディスク記録装置からディスク I D 信号を送り、画像データ等を暗号化するので、C A T V 会社は各ユーザに配信する暗号化コンテンツを個別に変える必要がなく、放送時のシステムを簡単にでき、低コストで、大量の視聴者に同じコンテンツを提供することができる。さらに本実施の形態によると C A T V デコーダを有する各ユーザ毎に R A M ディスク 1 枚だけに記録を許可することができる。

【 0 0 8 7 】

なお本実施の形態ではケーブルテレビからのコンテンツを放送する場合について説明したが、電波による放送でも同様である。

【 0 0 8 8 】

以下本発明の異なる実施の形態における暗号化コンテンツ記録再生方法について図面を参照しながら説明する。図 6 は本発明による第 3 の実施の形態における、BCA領域を有する書き換え型もしくは追記型の光ディスクである。

【 0 0 8 9 】

また図 7 は図 6 の光ディスクを用いて暗号化コンテンツを記録する際のブロッ

ク図である。なお、第1、第2の実施の形態と共通の部分は説明を簡略化する。

【0090】

図6において、601は書き換え型もしくは追記型の光ディスク（以下光ディスク）、602はディスク情報を凹凸ピットで記録してあるコントロールデータ領域、603はユーザがデータを記録するデータ領域、604はディスクIDを記録してあるBCA領域である。

【0091】

BCA領域604では、コントロールデータ領域102の内周部分の凹凸ピット上の記録膜が、606の様に半径方向に長い形状でかつ複数個、部分的にYAGレーザなどのパルスレーザでトリミングされている。

【0092】

なおトリミングはディスク製造者によって行われる。またディスクIDを付加することにより、光ディスクの管理を容易に実現することができる。さらにBCA領域が凹凸ピット上に記録されることにより、BCA領域内の光ディスクを識別する情報が容易に改ざんされることを防止することができる。

【0093】

さらにコントロールデータ領域602とBCA領域604が隣接していることにより、コントロールデータ領域602を再生する際に、BCA領域604も続けて再生することができる、もしくはBCA領域604を再生する際に、コントロールデータ領域602を続けて再生することができるので、例えば光ディスクを起動する際にCPUが速やかにディスクを識別するためのBCA領域604の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

【0094】

なお本実施の形態のBCA領域604は、コントロールデータ領域602の内周部分の凹凸ピット上の記録膜をトリミングしているが、書き換え型もしくは追記型の光ディスクを構成する記録膜は、再生専用の光ディスクにおける反射膜に対して熱による影響を受けやすい。コントロールデータ領域602の内周部分をトリミングすることにより、外周部分をトリミングする場合に比べて、トリミン

グの際に発生する熱からデータ領域 6 0 3 を保護することができる。

【 0 0 9 5 】

なおトリミング前の B C A 領域 6 0 4 に記録されているデータが、コントロールデータ領域 6 0 2 に記録されていても良い。B C A 領域 6 0 4 に記録されているデータが、コントロールデータ領域 6 0 2 にも記録されていることにより、トリミングを行ってもコントロールデータ領域 6 0 2 の前記データを保護することができる。

【 0 0 9 6 】

さらに前記データが B C A 領域 6 0 4 から、コントロールデータ領域 6 0 2 まで連続して繰り返し記録されている場合には、コントロールデータ領域 6 0 2 の前記データを見つけることによって、B C A 領域 6 0 4 の位置を予想することができる。

【 0 0 9 7 】

また 6 0 5 は鍵情報記録領域である。鍵情報記録領域 6 0 5 は、データ領域 6 0 3 と同じく光ビームを照射することにより記録される。

【 0 0 9 8 】

本実施の形態のように、コントロールデータ領域 6 0 2 と鍵情報記録領域 6 0 5 が隣接していることにより、コントロールデータ領域 6 0 2 を再生する際に、鍵情報記録領域 6 0 5 も続けて再生することができる、もしくは鍵情報記録領域 6 0 5 を再生する際に、コントロールデータ領域 6 0 2 を続けて再生することができるので、例えば光ディスクを起動する際に C P U が速やかにディスクを識別するための B C A 領域 6 0 4 の情報を入手し、暗号化されたコンテンツを再生するための処理を早めることが可能になる。

【 0 0 9 9 】

図 7 において、7 0 1 は C A T V 会社、7 0 2 は映画ソフト等のコンテンツ、7 0 3 は第 1 暗号鍵、7 0 4 は第 1 暗号化エンコーダ、7 0 5 は第 1 暗号化コンテンツ、7 0 6 は C A T V デコーダ、7 0 7 は鍵発行センター、7 0 8 は C A T V デコーダ 7 0 6 のシステム I D、7 0 9 はコンテンツ 7 0 2 のタイトルコード、7 1 0 は時間制限情報、7 1 3 は第 1 暗号デコーダ、7 1 4 は光ディスク記録

装置、715は光ディスク601のディスクID、716はコンテンツ702のタイトルコード、717は記録回路、719は鍵情報記録回路、720はBCA再生部、721はデータ再生部、722は第2暗号デコーダ、723は鍵情報再生部である。

【0100】

まずCATV会社701は、映画ソフト等のコンテンツ702を第1暗号鍵703を用いて第1暗号化エンコーダ704にて暗号化し、第1暗号化コンテンツ705を生成し、各ユーザのCATVデコーダ706に送信する。

【0101】

ここでコンテンツ702をC、第1暗号鍵703をFK、第1暗号化コンテンツ705をC[FK]とすると、 $C * FK = C[FK]$ と表記される。

【0102】

CATVデコーダ706はネットワークを介して鍵発行センター707へ、CATVデコーダ706のシステムID708と、視聴したい前記コンテンツのタイトルコード709を送る。

【0103】

なお、タイトルコード709はTVの画面に従って選択することにより入力しても良いし、直接キーボードから入力しても良いし、リモートコントローラー等から入力しても良い。従ってタイトルコード709は、ユーザが独自に入手していても良いし、第1暗号化コンテンツ705と共にCATVデコーダ706に送られてきても良いし、番組案内等の形態で第1暗号化コンテンツ705とは別の時間に予め送られていても良い。

【0104】

鍵発行センター707は、CATVデコーダ706のシステムID708、前記コンテンツのタイトルコード709、時間制限情報710に対応する鍵K712をCATVデコーダ706の第1暗号デコーダ713へネットワークを介して送信する。

【0105】

なお時間制限情報710により、同一のコンテンツを時間を変えて複数回放送



する場合を区別することができる。

#### 【0106】

ここで第1復号鍵をFK、CATVデコーダ706のシステムID708をDID、時間制限情報710をTIME、コンテンツのタイトルコード709をTとすると、鍵Kは、 $FK = K * T * DID * TIME$ の関係を満たしている。

#### 【0107】

第1暗号デコーダ713は鍵K712と、前記コンテンツのタイトルコード709と、システムID708に加えて、時間情報725が時間制限情報710の条件を満たしていれば、第1暗号化コンテンツ705を復号し、映像信号の場合は、デスクランブルされた信号が出力され、TVで視聴できる。復号化処理を式で表すと、 $C[FK] \# (K * T * DID * TIME) = C[FK] \# FK = C$ となる。

#### 【0108】

次に前記コンテンツを光ディスク601に記録する方法を説明する。光ディスク601へ記録する際には、CATVデコーダ706にて復号化されていない、第1暗号化コンテンツ705が光ディスク記録装置714に送られ、記録回路717により例えば8-16変調により変調されて、図示されていない光ピックアップにより光ディスク601に記録される。

#### 【0109】

従って光ディスク601に暗号化されて記録された前記コンテンツを再生するためには、第1暗号化コンテンツ705を復号する必要がある。

#### 【0110】

光ディスク記録装置714はネットワークを介して鍵発行センター707へ、光ディスク601のディスクID715と、再生したい前記コンテンツのタイトルコード716を送る。

#### 【0111】

なおディスクID715を送るタイミングは、鍵発行センター707とアクセスする際に送っても良いし、視聴の際に、タイトルコードと一緒に送っても良い。

【0112】

またディスクIDの送信方法も、図7に示すように光ディスク601のBCA領域604を再生して、BCA再生部720の出力信号を直接鍵発行センター707に送る以外にも、例えばディスク起動時等の、鍵発行センター707とのアクセス以前にBCA領域604を再生して、光ディスク記録装置714やCATVデコーダ706に保管しておき前記タイミングで鍵発行センター707に送っても良い。

【0113】

さらにディスクIDが、ラベル等の形態で視覚的にも認識できる場合には、キーボードから入力しても良いし、ラベルがバーコードになっている場合にはバーコードリーダーから読みとって良い。

【0114】

鍵発行センター707は、光ディスク601のディスクID715、コンテンツのタイトルコード716に対応する鍵DK718を、光ディスク記録装置714の暗号記録回路719へ送信する。

【0115】

ここで第1復号鍵をFK、光ディスク601のディスクID715をBCA、コンテンツのタイトルコード716をTとすると、鍵DKは、 $FK = DK * BCA * T$ の関係を満たしている。

【0116】

光ディスク記録装置714の鍵情報記録回路719に入力された鍵DKは、例えば8-16変調により変調されて、光ピックアップにより光ディスク601の鍵情報記録領域605に記録される。

【0117】

なお鍵DKは鍵情報記録領域605に、同じ鍵が複数個記録されても良い。同じ鍵が複数個記録されることにより、鍵情報記録領域605の記録膜が劣化した場合や、傷がついた場合に鍵DKを保護することができる。

【0118】

また本実施の形態では、鍵情報記録領域605はデータ領域603の内周側に

設けられているが、データ領域 603 の外周側にあっても良く、内周側と外周側の両方に設けられていても良い。外周側に設けられることにより、より多くの鍵 DK を記録することが可能となる。また鍵情報記録領域が複数個、分散して設けられることにより、一つの鍵情報記録領域が再生できなくなった場合でも、他の鍵情報記録領域により鍵 DK を保護することができる。

## 【0119】

一方、光ピックアップから出力されるレーザ光が光ディスク 601 の前記コンテンツが記録された領域を照射し、その反射光がデータ再生部 721 に入力され、データ再生部 721 は暗号化された信号を出力し、出力信号は第 2 暗号デコーダ 722 に入力される。

## 【0120】

さらに光ピックアップから出力されるレーザ光は光ディスク 601 の BCA 領域 604 を照射し、その反射光が BCA 再生部 720 に入力され、BCA 再生部 720 はディスク ID 信号 715 を出力し、出力信号は暗号デコーダ 722 に入力される。

## 【0121】

さらに、光ピックアップから出力されるレーザ光は光ディスク 601 の鍵情報記録領域 605 を照射し、その反射光が鍵情報再生部 723 に入力され、鍵情報再生部は鍵 DK を出力し、出力信号は第 2 暗号デコーダ 722 に入力される。

## 【0122】

なお、鍵発行センター 707 とアクセスしてすぐに再生する際は、鍵情報記録回路 719 は、鍵 DK を鍵情報記録領域 605 に記録する前に、直接第 2 暗号デコーダに入力しても良い。この様にすることにより、再生を開始するまでの時間を短縮することができる。

## 【0123】

暗号デコーダ 722 では、入力されたディスク ID 信号 715 と、鍵 DK と、前記コンテンツのタイトルコード 716 からなる復号鍵により、暗号化された信号の復号を行う。復号化処理を式で表すと、 $C[FK] \# (DK * BCA * T) = C[FK] \# FK = C$  となる。コンテンツが映像情報の場合は例えば MPEG

信号が伸長されて、映像信号が得られる。

【0 1 2 4】

鍵発行センター 7 0 7 から鍵信号を受け取る時に課金されたとすると、本実施の形態によると、視聴するときと、光ディスク 6 0 1 に記録したコンテンツを初めて再生するときとに別々に課金され、光ディスク 6 0 1 に記録しただけでは課金されない。

【0 1 2 5】

従って、視聴と光ディスク 6 0 1 への記録の両方に対してまとめて課金する場合に対して、視聴はしたいが光ディスク 6 0 1 に記録する必要がないユーザや、光ディスク 6 0 1 に記録したいが、放送されるときに視聴する必要がないユーザにとっては課金される金額を安くすることができる。

【0 1 2 6】

また光ディスク 6 0 1 に記録しただけでは課金されないので、ユーザは視聴した後で、再度視聴するために光ディスク 6 0 1 を再生するための鍵を受け取るかどうかを決定することができる。

【0 1 2 7】

なお、鍵 DK は鍵発行センター 7 0 7 からネットワークにより受け取る以外にも、コンテンツのタイトルとディスク ID 番号を電話等で口頭で伝えることにより、口頭で受け取ってキーボードから入力しても良い。

【0 1 2 8】

次に、鍵情報記録領域 6 0 5 に鍵 DK が記録された光ディスク 6 0 1 を鍵発行センター 7 0 7 とのアクセス終了後に再生する場合について説明する。

【0 1 2 9】

まず、光ピックアップから出力されるレーザ光が光ディスク 6 0 1 の前記コンテンツが記録された領域を照射し、その反射光がデータ再生部 7 2 1 に入力され、データ再生部 7 2 1 は暗号化された信号を出力し、出力信号は第 2 暗号デコーダ 7 2 2 に入力される。

【0 1 3 0】

一方、光ピックアップから出力されるレーザ光は光ディスク 6 0 1 の B C A 領域 6 0

4を照射し、その反射光がBCA再生部720に入力され、BCA再生部720はディスクID信号715を出力し、出力信号は第2暗号デコーダ722に入力される。

【0131】

さらに、光ピックアップから出力されるレーザ光は光ディスク601の鍵情報記録領域605を照射し、その反射光が鍵情報再生部723に入力され、鍵情報再生部は鍵DKを出力し、出力信号は第2暗号デコーダ722に入力される。

【0132】

第2暗号デコーダ722では、入力されたディスクID信号715と、鍵DKと、前記コンテンツのタイトルコード716からなる復号鍵により、暗号化されたコンテンツの復号を行う。復号化処理を式で表すと、 $C[FK] \# (DK * BCA * T) = C[FK] \# FK = C$ となる。コンテンツが映像情報の場合は例えばMPEG信号が伸長されて、映像信号が得られる。

【0133】

鍵情報記録領域605に鍵DKが一度記録されることにより、鍵発行センター707とのアクセスをすることなく、いつでも前記暗号化コンテンツを再生することができる。

【0134】

また、復号化処理に必要な復号鍵は全て光ディスク601に記録されているので、前記光ディスク601は、BCA再生部、鍵情報再生部、第2暗号デコーダを有する任意の光ディスク記録装置で再生することができる。

【0135】

また前記暗号化コンテンツをディスクIDの異なる光ディスクにコピーして再生しようとした場合には、BCA再生部から前記光ディスク601とは異なるディスクID信号が出力されるので、暗号化されたコンテンツを復号することができず、コンテンツはコピーされても再生されない。

【0136】

ただこの場合にも、コンテンツのタイトルとディスクIDをネットワークもしくは口頭で鍵発行センターに伝えることにより、課金の後、復号鍵を受け取って

も良い。このように、暗号化されたコンテンツを別の光ディスクにコピーされても、不正に再生されることはなく、暗号化されたコンテンツをコピーした光ディスクを再生するには必ず課金が伴うことから著作権を保護することができる。

## 【0137】

図8にシステムID、ディスクIDが異なる場合の第1暗号デコーダ713に入力される鍵K、鍵情報記録回路719に入力される鍵DKを整理する。図8において、T1、T2、T3は異なるコンテンツのタイトルコード、FK1、FK2、FK3はそれぞれタイトルコードがT1、T2、T3の暗号化コンテンツを復号するための復号鍵である。

## 【0138】

DID1、DID2、DID3はそれぞれ異なるCATVデコーダのシステムIDであり、BCA1、BCA2、BCA3はそれぞれ異なる光ディスクのディスクIDである。

## 【0139】

このとき、CATVデコーダに入力される鍵 $K_{mn}$ は、 $FK_n = K_{mn} * T_n * DID * TIME_n$ を満足するように決定され、光ディスク記録装置に入力される鍵DKは、 $FK_n = DK_{mn} * BCA_m * T_n$ を満足するように決定される。

## 【0140】

図8に示す様に、コンテンツが異なるときはもちろんのこと、コンテンツが同じ場合でも、異なるCATVデコーダ、異なるディスク、異なる放送時間ごとに鍵発行センターから入手する鍵情報は異なることから細部にわたる著作権の保護が可能になる。

## 【0141】

同様に、コンテンツが同じでもシステムID、ディスクID、時間情報が異なれば鍵情報が異なることから、CATV会社701は、ユーザごとに暗号化コンテンツを変える必要がなく、1つのコンテンツに対して1つの暗号化コンテンツを準備すれば良い。これにより放送時のシステムを簡単にでき、低コストで、大量の視聴者へのコンテンツの提供が可能になる。

【0 1 4 2】

なお本実施の形態ではケーブルテレビからのコンテンツを放送する場合について説明したが、電波による放送でも同様である。

【0 1 4 3】

【発明の効果】

本実施の形態の書き換え型もしくは追記型の光ディスクにより、従来の光ディスクに、前記光ディスクを識別する情報を付加することで、光ディスクの管理を容易に実現することができる。

【0 1 4 4】

また本実施の形態の暗号化データの記録方法により、世の中に 1 枚しか存在しない、光ディスクを識別する情報により暗号化することにより、光ディスクの不正なコピーを防止し、1 枚の光ディスクにしか同じ暗号化コンテンツの記録ができないため、著作権が保護できるという効果がある。

【0 1 4 5】

また本実施の形態の書き換え型もしくは追記型の光ディスクにより、暗号化されて記録されたデータを解読する際に鍵情報が必要なシステムにおいて、鍵情報記録領域に鍵情報が一度記録されることにより、再生する度に鍵情報を入手する必要がなくなるという効果がある。

【0 1 4 6】

また本実施の形態の暗号化データの記録方法により、暗号化されたコンテンツをコピーされても、不正に再生されることはなく、さらに復号化されたコンテンツが複製される際には必ず課金が伴うことから著作権を保護することができる。

【0 1 4 7】

また本実施の形態の暗号化データの記録方法により、コンテンツが同じでもシステム ID、ディスク ID、時間情報が異なれば鍵情報が異なることから、CATV 会社 7 0 1 は、ユーザごとに暗号化コンテンツを変える必要がなく、1 つのコンテンツに対して 1 つの暗号化コンテンツを準備すれば良く、これにより放送時のシステムを簡単にでき、低コストで、大量の視聴者へのコンテンツの提供が可能になる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施の形態における光ディスクの平面図

【図 2】

本発明の第 1 の実施の形態における B C A 領域を再生したときの光ディスク記録装置の出力信号の説明図

【図 3】

本発明の第 1 の実施の形態における B C A 再生部のブロック図

【図 4】

本発明の第 1 の実施の形態における暗号化コンテンツの記録方法のブロック図

【図 5】

本発明の第 2 の実施の形態における暗号化コンテンツの記録方法のブロック図

【図 6】

本発明の第 3 の実施の形態における光ディスクの平面図

【図 7】

本発明の第 3 の実施の形態における暗号化コンテンツの記録方法のブロック図

【図 8】

本発明の第 3 の実施の形態における、システム I D、ディスク I D が異なる場合の鍵情報の整理のための図

【符号の説明】

1 0 1 光ディスク

1 0 2 コントロールデータ領域

1 0 3 データ領域

1 0 4 B C A 領域

3 0 1 光ピックアップ

4 0 1 B C A 再生部

4 0 8 暗号化エンコーダ

4 1 2 データ再生部

4 1 3 暗号デコーダ

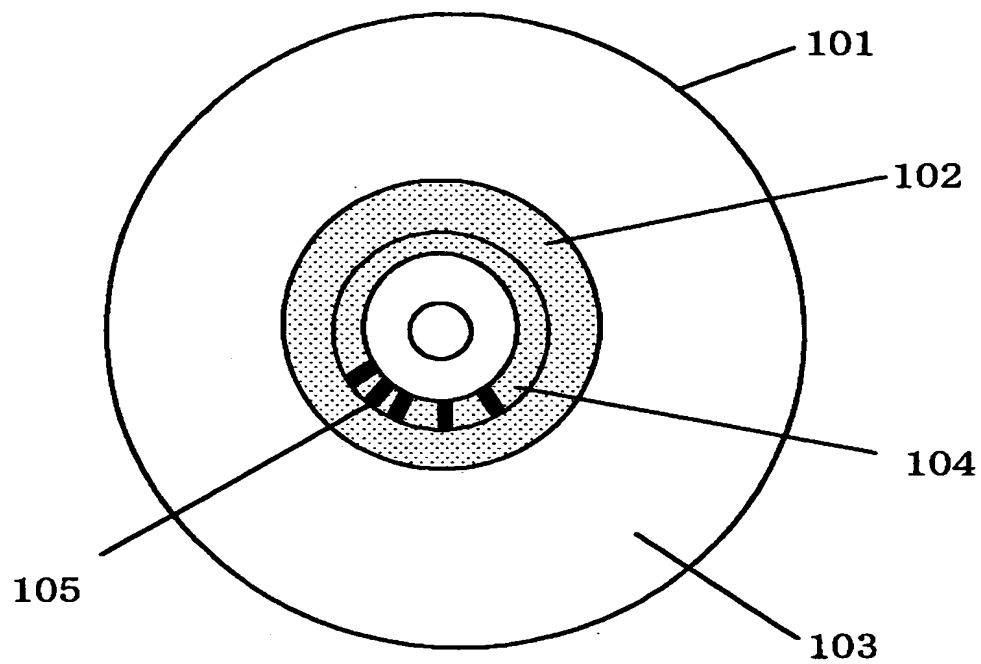


5 0 8 システム I D  
5 2 3 会社識別信号  
6 0 5 鍵情報記録領域  
7 1 9 鍵情報記録回路  
7 2 3 鍵情報再生部

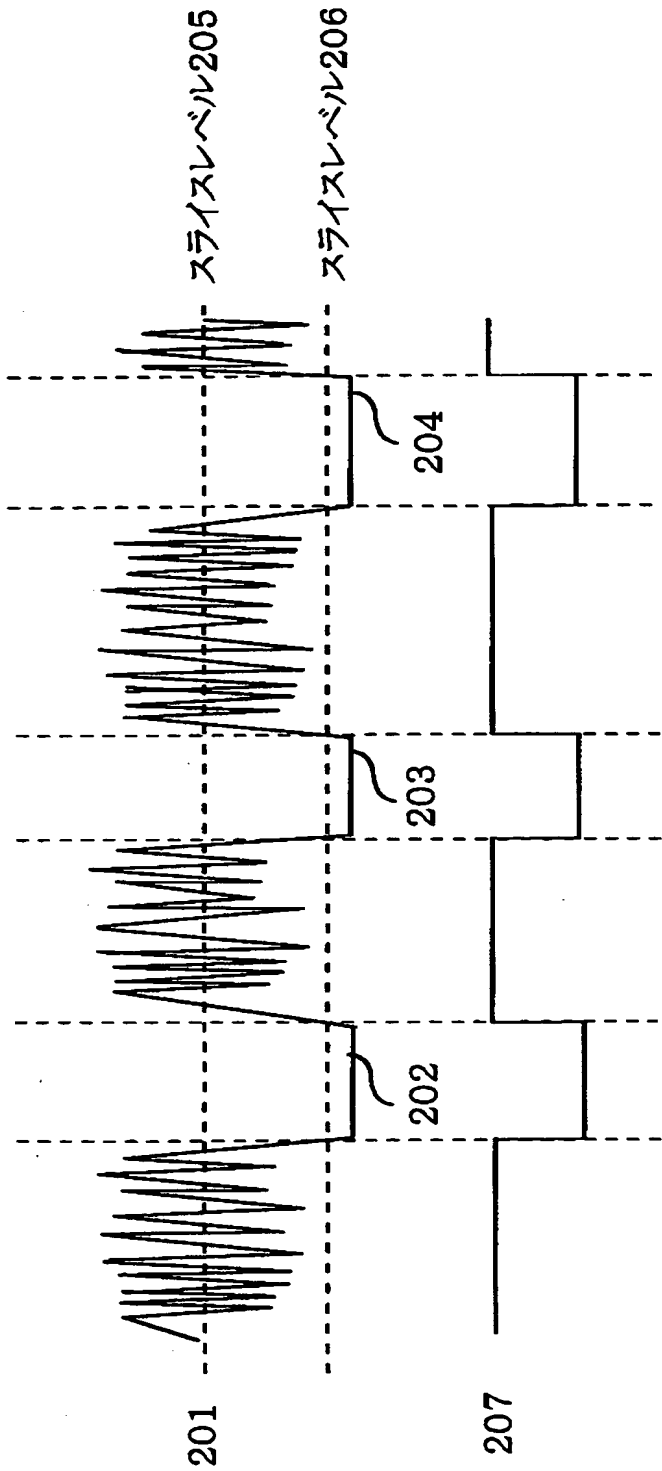
【書類名】

図面

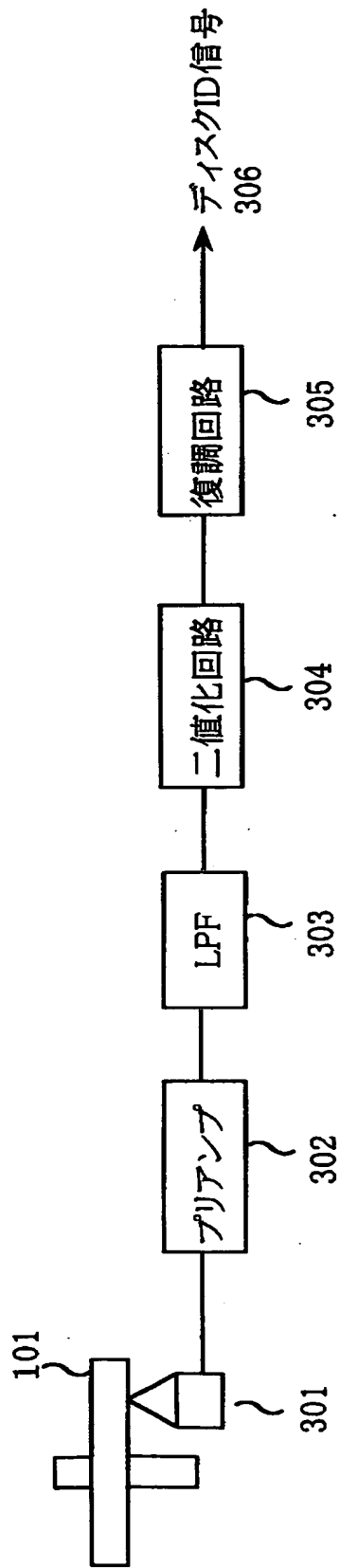
【図 1】



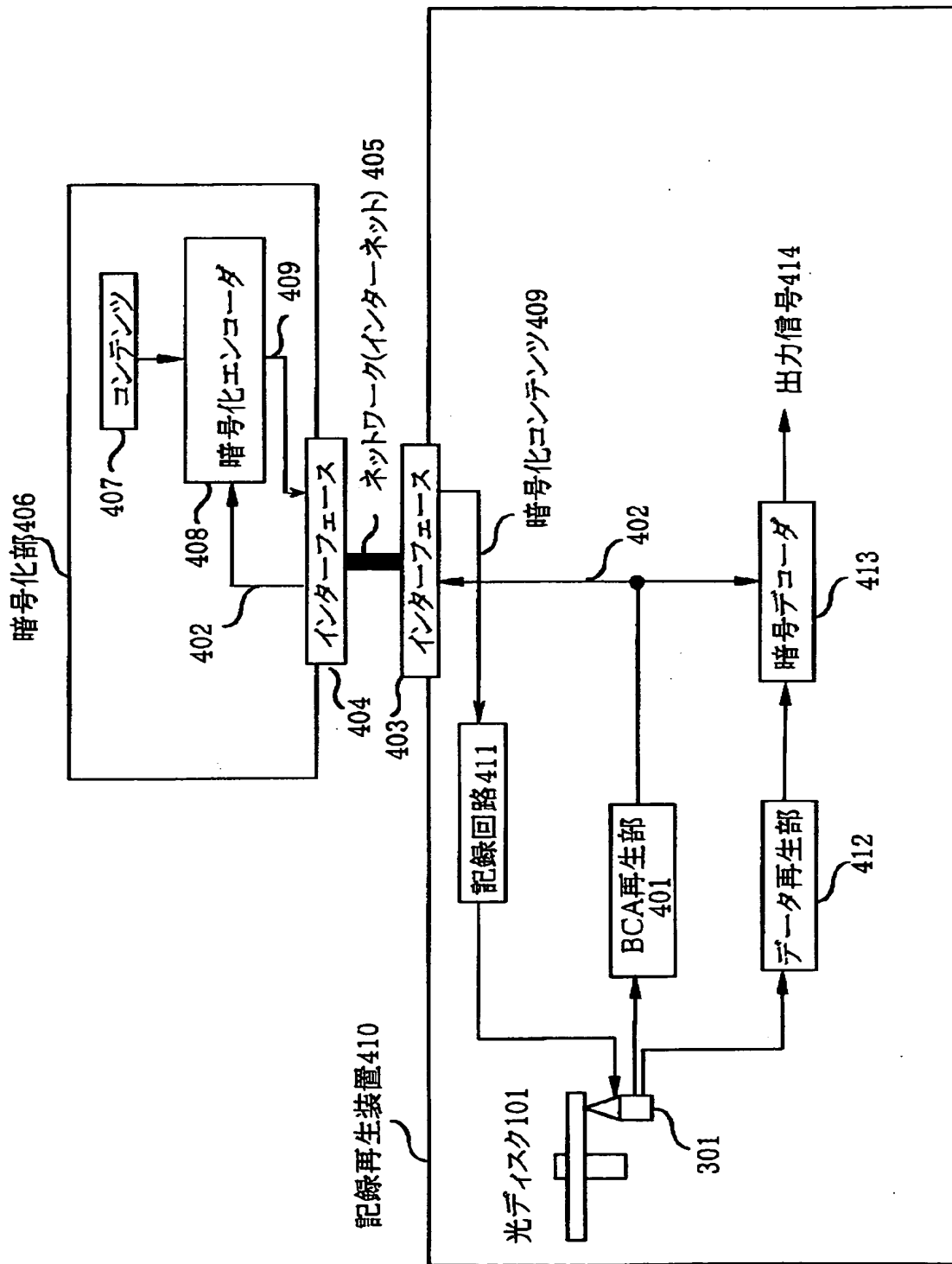
【図 2】



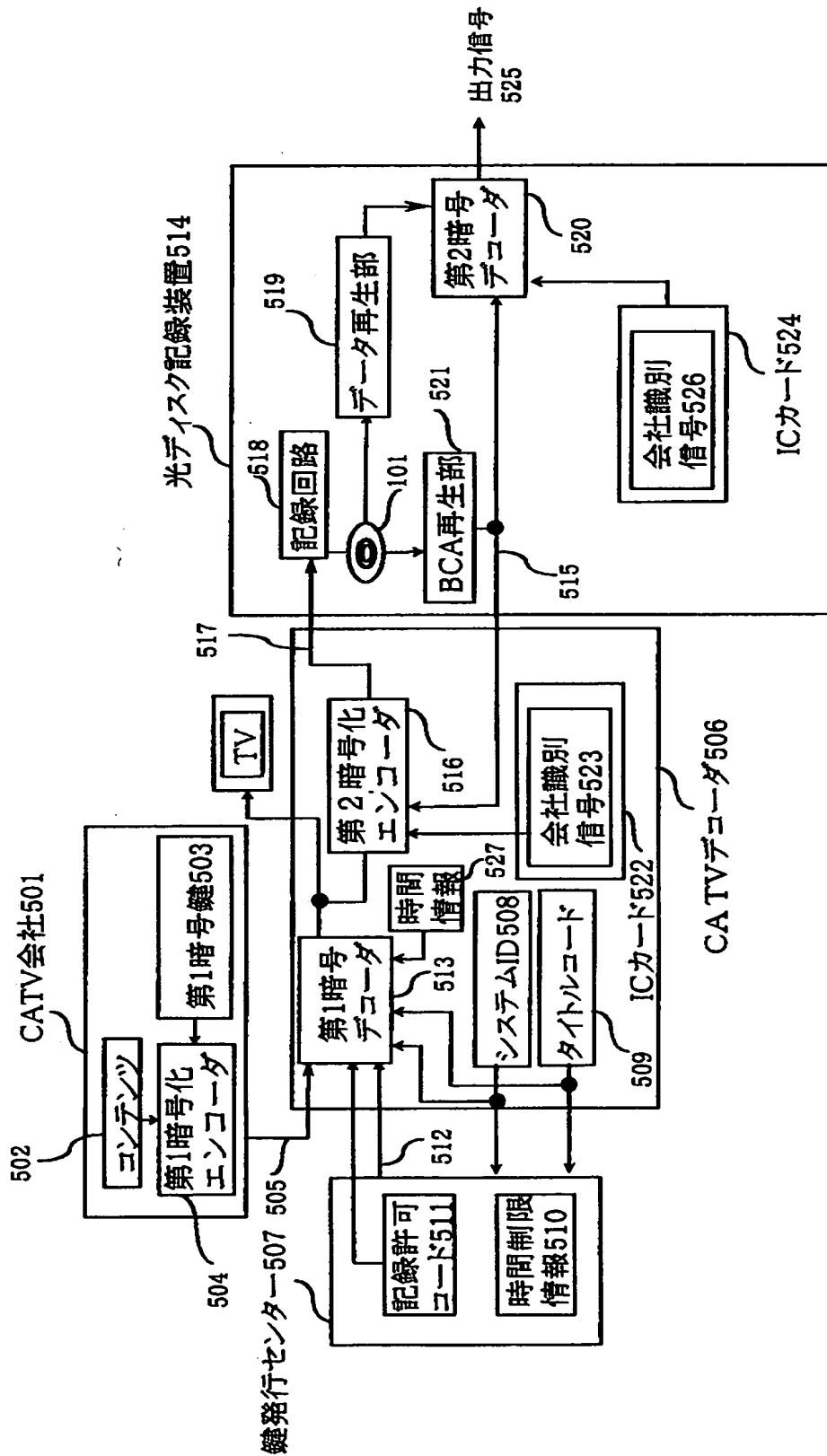
【図 3】



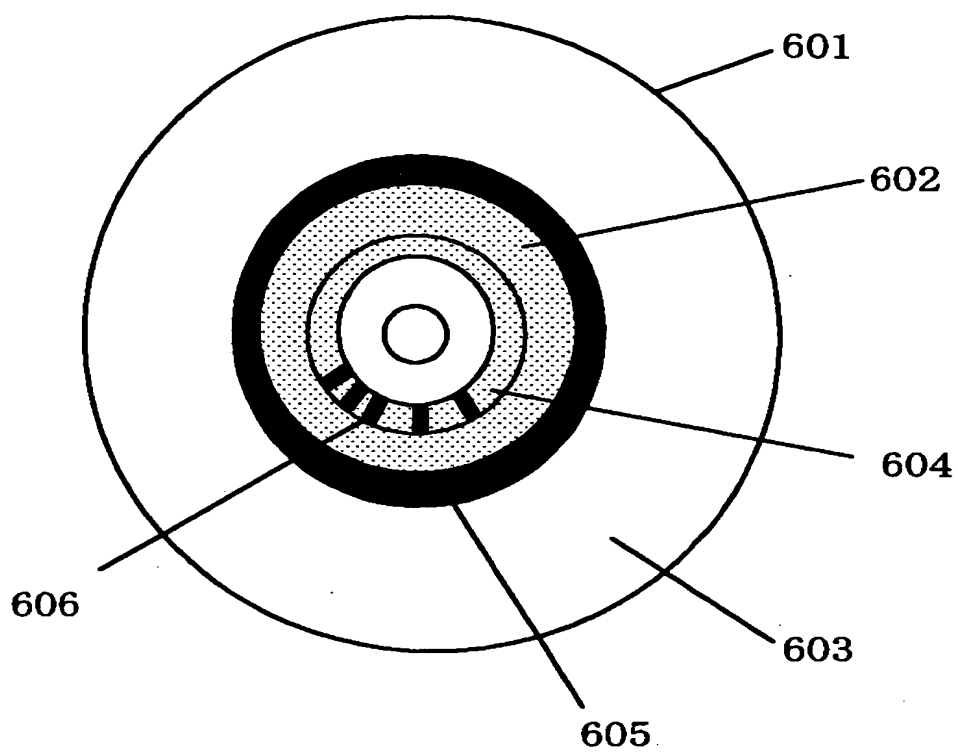
【図 4】



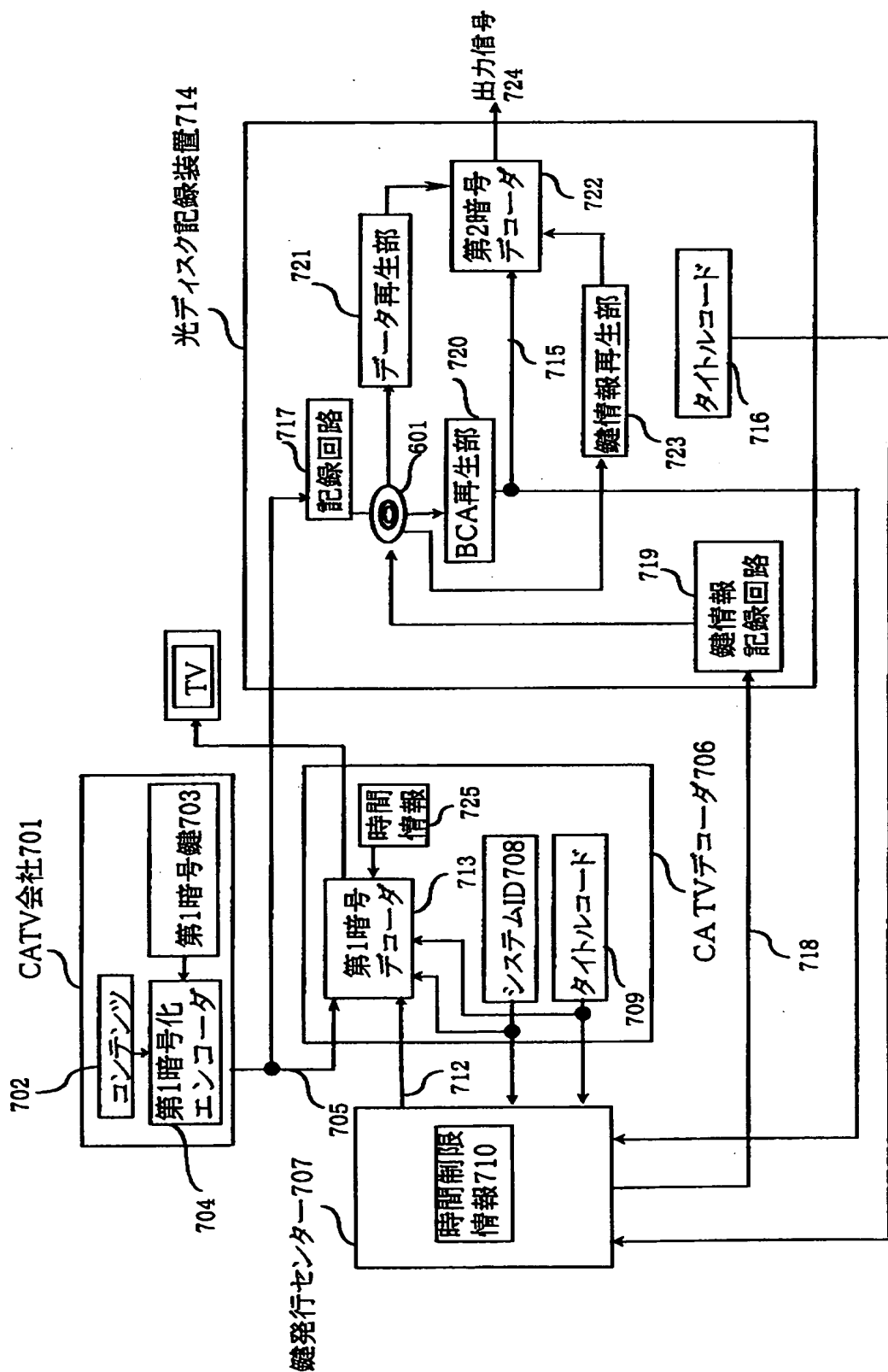
【図 5】



【図 6】



【图7】





【図 8】

タイトルコードT		T1	T2	T3
第1復号鍵FK		FK1	FK2	FK3
TIME		TIME1	TIME2	TIME3
システムID	DID1	K11	K12	K13
	DID2	K21	K22	K23
	DID3	K23	K32	K33
ディスクID	BCA1	DK11	DK12	DK13
	BCA2	DK21	DK22	DK23
	BCA3	DK31	DK32	DK33

【書類名】 要約書

【要約】

【課題】 簡単なシステムで、不正コピーを防止しつつ、ネットワークもしくは電波により発信されたコンテンツを光ディスクへ記録するための、暗号化コンテンツ記録方法を提供することを目的とする。

【解決手段】 ディスクの種類等を凹凸ピットで記録してあるコントロールデータ領域 1 0 2、ユーザがデータを記録するデータ領域 1 0 3、コントロールデータ領域 1 0 2 の内周部分の凹凸ピット上の記録膜を Y A G レーザなどのパルスレーザでトリミングすることにより、ディスク I D 信号を記録してある B C A 領域 1 0 4 を有し、ディスク I D 信号が暗号を解く復号鍵となるように暗号化されたコンテンツをデータ領域 1 0 3 に記録する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社